The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/27/2011

SUBJECT:
Multiple Vulnerabilities in Novell GroupWise Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Novell GroupWise that could allow an attacker to take complete control of a vulnerable system. Novell GroupWise is a collaborative software product that includes email, calendars, instant messaging, and document management. Successful exploitation of four of these vulnerabilities could result in an attacker gaining system level privileges on the affected system. The attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Failed exploit attempts of these four vulnerabilities may result in a denial of service condition. The remaining vulnerabilities could allow for information disclosure.

SYSTEMS AFFECTED:
- Novell GroupWise 8
- Novell GroupWise 8 Internet Agent
- GroupWise 8.0x up to (and including) 8.02HP2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

DESCRIPTION:
Multiple vulnerabilities have been discovered in Novell GroupWise that could allow an attacker to take complete control of a vulnerable system. Details of these vulnerabilities are as follows:

Novell GroupWise Internet Agent (GWIA) Stack Buffer Overflow Vulnerability

Novell GroupWise Internet Agent (GWIA) is prone to a buffer overflow vulnerability because it fails to parse the yearly and weekly 'calendar recurrence ('RRULE') variable included in a 'VCALENDAR' message. A successful attack may allow aremote attacker to execute arbitrary code with SYSTEM-level privileges. Authentication is not required in order to exploit this vulnerability.

Novell GroupWise Internet Agent HTTP Interface Stack Buffer Overflow Vulnerability

Novell GroupWise Internet Agent is prone to a stack-based buffer overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data to the HTTP interface. Successful exploits could allow attackers to execute arbitrary code in the context of the application.

Novell GroupWise 8 WebAccess 'Directory.Item' Parameters Cross-Site Scripting Vulnerabilities

Novell GroupWise WebAccess is prone to multiple cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied input to the 'Directory.Item.name' and 'Directory.Item.displayName' parameters. Successful exploits will allow attackers to insert arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This will allow the attacker to steal cookie-based authentication credentials or launch other attacks.

Novell GroupWise Internet Agent (GWIA) TZNAME Variable Parsing Remote Code Execution Vulnerability

Novell GroupWise Internet Agent is prone to a buffer overflow vulnerability because it fails to parse the time zone description (TZNAME) variable included in a 'VCALENDAR' message. A successful attack may allow a remote attacker to execute arbitrary code with SYSTEM-level privileges. Authentication is not required in order to exploit this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Novell to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Novell:

http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7009216&sliceId=1&docTypeID=DT_TID_1_1calendar&dialogID=268451098&stateId=0%200%20268449338
http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7009215&sliceId=1&docTypeID=DT_TID_1_1&dialogID=268451081&stateId=0%200%20268449329
http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7009210&sliceId=1&docTypeID=DT_TID_1_1&dialogID=26844393
http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7009214&sliceId=1&docTypeID=DT_TID_1_1&dialogID=268451061&stateId=0%200%20268449323
http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7009208&sliceId=1&docTypeID=DT_TID_1_1&dialogID=268443893&stateId=0%200%20268449181

Security Focus:

http://www.securityfocus.com/bid/49781
http://www.securityfocus.com/bid/49777
http://www.securityfocus.com/bid/49779
http://www.securityfocus.com/bid/49773
http://www.securityfocus.com/bid/49774

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2662
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2663
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0334
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2661
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0333